WHAT IS CLAIMED IS:

1. A method of authenticating a device, the method comprising:

receiving a certificate from the device, the certificate including a plurality of fields, including a field holding a digital signature from a certifying authority;

verifying the digital signatures in the certificate, the verifying including at least one of:

verifying the certifying authority digital signature using the certifying authority public key; and

verifying a device digital signature using a device public key ; and

receiving validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria; and

if the digital signatures are verified and validated, transmitting a session key to the device to establish a secure communication channel.

2. The method of claim 1 wherein the source is one of a portable medium and firmware.

3. The method of claim 1 wherein the device is one of an engine, a device that embeds an engine, a third party digital rights management protocol, an application running in an open computing environment, and a clearinghouse server, the certificate identifying one or more secure application programming interfaces (APIs) for which an application operable with the device may have access.

4. The method of claim 1 wherein the certificate is digitally signed by a private key assigned according to a class of device, the class of device including engines, device devices embedding an engine with no external digital input/output port, device devices embedding an engine with digital input/output ports, device applications not embedding an engine, third party digital rights management protocols, and clearinghouse servers.

5. The method of claim 1 wherein the certifying of the device includes certifying a second host for a host to second host secure communication channel, the certifying allowing a copy function between the host and the second host.

6. The method of claim 1 wherein the data in the certificate specifies one or more of a product category, a product line, a model, a revision and a serial number of the device.

7. The method of claim 6 wherein the source validation data is compared with the data in the certificate to identify as invalid one or more of the product category, the product line, the model, the revision and the serial number of the device.

8. The method of claim 1 wherein the certificate includes one or more of a certifying authority identifier field, a version field, a sign key identifier field, an exposed methods field, a company field, a model identifier field, a revision field, a metadata identifier field, a device digital signature key field, a certifying authority digital signature field, a serial number field, a protocol public key field and a device digital signature field, wherein the certifying authority digital signature verifies one or more of the fields in the certificate and the device digital signature verifies one or more of the fields in the certificate.

09940026 .082701

9. The method of claim 1 wherein the certificate enables an entity receiving the certificate to control the quality of the device by invalidating devices that are false or have latent defects.

10. The method of claim 6 wherein the certificate further includes fields provided by a device manufacturer, including the company public key, wherein the company public key is digitally signed by the certifying authority.

11. The method of claim 6 wherein the certificate further includes fields provided by a device manufacturer, the fields including the device public key, wherein the device public key is digitally signed by the company.

12. The method of claim 6 wherein one or more of the product category, the product line, the model, the revision and the serial number of the device are provided to a certificate creator after the device passes a qualification procedure.

13. The method of claim 1 wherein the certificate specifies one or more certificate classes, the certificate classes providing a set of methods that may be exposed after the transmitting the session key.

14. The method of claim 13 wherein the set of methods includes digital rights management (DRM) methods include one or more of a copy method, a record method, a play method, a read secure metadata method, a write secure metadata method, and an unlock method, the DRM methods operable according to a type of the device.

15. The method of claim 14 wherein:

the unlock method is associated with a clearinghouse server;

the copy method is associated with one of an engine and a first DRM application operable with a second DRM application; and

the record method is associated with one or more of a player, a mastering tool, a kiosk, and a clearinghouse server.

16. The method of claim 1 wherein each of the fields hold 326-bit values for 163-bit elliptic curve cryptography.

17. The method of claim 1 wherein the certifying authority public key is referenced by a field of the certificate.

18. The method of claim 1 wherein the certifying authority public key is in the firmware component.

19. An apparatus for certifying a device, the apparatus comprising:

means for receiving a certificate request from the device, the certificate request including a plurality of fields, including a field holding a protocol public key;

means for verifying digital signatures in the certificate, the verifying including at least one of:

verifying the certifying authority digital signature using the certifying authority public key; and verifying a device digital signature using a device public key in the certificate; and

means for receiving validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria; and

means for transmitting a session key to the device to establish a secure communication channel when the digital signatures are verified and validated.

20. An engine configured to certify a host, the engine comprising:

a firmware component including:

a block configured to receive a certificate from the host, the certificate including a plurality of fields, including a field holding a protocol public key;

a block configured to verify one or more digital signatures in the certificate, including at least one of:

a certifying authority digital signature using a certifying authority public key; and

a device digital signature using a device public key in the certificate; and

a block configured to receive validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria; and

a block configured to transmit a session key to the host to establish a secure communication channel when the digital signatures are verified and validated.

21. A computer program product, the computer program product comprising:

signal bearing media bearing digital information holding a firmware component, the firmware component including:

a block configured to receive a certificate from the device, the certificate including a plurality of fields, including a field holding a protocol public key;

a block configured to verify digital signatures in the certificate, including at least one of:

a certifying authority digital signature using the certifying authority public key; and a device digital signature using a device public key in the certificate; and

a block configured to receive validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria; and

a block configured to transmit a session key to the device to establish a secure communication channel when the digital signatures are verified and validated.

22. The computer program product of claim 21 wherein the certifying authority public key is referenced by a field of the certificate.

23. The computer program product of claim 21 wherein the certifying authority public key is in the firmware component.

09540026 .082701